(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 946 018 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.09.1999 Bulletin 1999/39

(51) Int. Cl.[6]: **H04L 9/30**

(21) Application number: **99105099.8**

(22) Date of filing: **25.03.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **26.03.1998 JP 7983698**
21.08.1998 JP 23608798

(71) Applicant:
Nippon Telegraph and Telephone Corporation
Tokyo (JP)

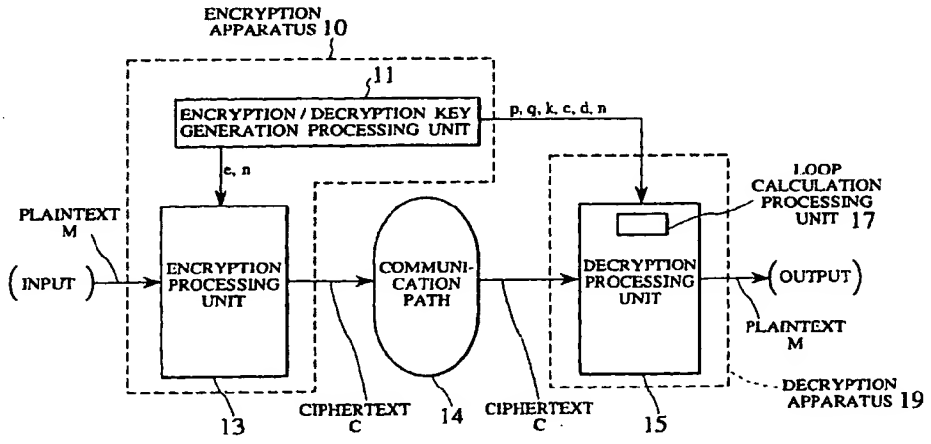
(72) Inventors:
- **Takagi, Tsuyoshi,**
  c/o NIPPON TELEGRAPH AND
  Shinjuku-ku, Tokyo 163-14 (JP)
- **Naito, Shozo,**
  c/o NIPPON TELEGRAPH AND
  Shinjuku-ku, Tokyo 163-14 (JP)

(74) Representative: **HOFFMANN - EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) Scheme for fast realization of encryption, decryption and authentication

(57) A new scheme for fast realization of encryption, decryption and authentication which can overcome the problems of the RSA cryptosystem is disclosed. The encryption obtains a ciphertext C from a plaintext M according to $C \equiv M^e \pmod{n}$ using a first secret key given by N (≥ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy $ed = 1 \pmod{L}$ where L is a least common multiple of p_1-1, p_2-1, ·····, p_N-1. The decryption recovers the plaintext M by obtaining residues $M_{p\,1\,k\,1}$, $M_{p\,2\,k\,2}$, ·····, $M_{p\,N\,k\,N}$ modulo p_1^{k1}, p_2^{k2}, ·····, p_N^{kN}, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key $p_1, p_2, \cdots\cdots\cdots, p_N$, and by applying the Chinese remainder theorem to the residues $M_{p\,1\,k\,1}, M_{p\,2\,k\,2}, \cdots\cdots\cdots, M_{p\,N\,k\,N}$. This encryption/decryption scheme can be utilized for realizing the authentication.

FIG. 1



EP 0 946 018 A2

Description

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] The present invention relates to a scheme for fast realization of encryption, decryption and authentication which is suitable for data concealment and communicating individual authentication in communications for a digital TV, a pay-per-view system of the satellite broadcast, a key distribution in the information distribution, electronic mails, electronic transactions, etc.

DESCRIPTION OF THE BACKGROUND ART

[0002] In recent years, in the field of communications, various types of cryptographic techniques have been proposed because the cryptographic technique can be effectively used for the protection of secrecy between communicating parties such as the concealment of information to be transmitted. The performances of such a cryptographic technique can be evaluated in terms of the security level of cryptosystem and the speed of encryption/decryption. Namely, the cryptosystem for which the security level is high and the encryption/decryption speed is high is a superior cryptosystem.

[0003] Among such cryptographic techniques, there is a type of public key cryptosystem that uses the modular exponent calculations, known as RSA (Rivest Shamir Adleman) cryptosystem, which is already in practical use. In this RSA cryptosystem, it has been shown that the plaintext can be obtained from the ciphertext if the prime factoring of the public key can be made (see R. Rivest, A. Shamir and L. Adleman; "A method for obtaining digital signatures and public-key cryptosystems", Comm. ACM, Vol. 21, No. 2, pp. 120-126 (1978)).

[0004] The public key cryptosystem such as RSA cryptosystem has its security based on the computational difficulty for obtaining the secret key from the public key which is a publicly disclosed information, so that the security level can be increased as much when a size of the public key is increased. On the other hand, the RSA cryptosystem has been associated with a drawback that it requires a considerable amount of time for encryption/decryption because it carries out higher degree modular exponent calculations and therefore the required amount of calculations is large.

[0005] The encryption/decryption can be made faster by reducing the degree of the modular exponent calculations, for example, but that will require the reduction of the size of the public key and that in turn causes the lowering of the cryptosystem security.

[0006] In the following, the RSA cryptosystem will be described in further detail.

[0007] First, mutually different arbitrary prime numbers p and q are set as the first secret key, and the first public key n is obtained as:

$$n = pq$$

while the least common multiple L of (p-1) and (q-1) is obtained as:

$$L = \mathrm{lcm}\,(p-1, q-1).$$

[0008] Then, an arbitrary integer e is set as the second public key, and the second secret key d given by:

$$ed \equiv 1 \pmod{L}$$

is obtained using the Euclidean division algorithm.

[0009] Then, a plaintext M and its ciphertext C can be expressed as follow:

$$C \equiv M^e \pmod{n},$$

$$M \equiv C^d \pmod{n}.$$

[0010] Here, the value of the second public key e can be rather small like 13, for instance, so that the encryption processing can be made very fast, but the value of the second secret key d has a size nearly equal to n so that the decryption processing will be quite slow.

[0011] On the other hand, the processing amount of the modular exponent calculations is proportional to the cube of the size of a number, so that by utilizing this property, the Chinese remainder theorem can be used in order to make the decryption processing faster.

[0012] The decryption processing using the Chinese remainder theorem proceeds as follows.

$$d_p \equiv d \pmod{p-1},$$

$$d_q \equiv d \pmod{q-1},$$

$$uq \equiv 1 \pmod{p},$$

$$M_p \equiv C^{dp} \pmod{p},$$

$$M_q \equiv C^{dq} \pmod{q},$$

$$M \equiv ((M_p - M_q)u \pmod{p})q + M_q,$$

where u is an inverse of q modulo p.

[0013] Here, the size of each of p, q, d_p and d_q is a half of the size of n so that the modular exponent calculations module p or q can be processed eight times faster, and as a result, the decryption processing as a whole can be made four times faster.

[0014] Also, the RSA cryptosystem can be easily cryptoanalyzed if the prime factoring of n can be made. Currently, the potentially threatening prime factoring algorithms include the number field sieve method and the elliptic curve method.

[0015] The required amount of calculations is of a quasi-exponential order of the size of n in the number field sieve method and of a quasi-exponential order of the size of a prime number in the elliptic curve method. The elliptic curve method is practically not a problem because of its high order calculations and large coefficients. On the other hand, the number field sieve method has a record for the prime factoring of the largest number realized so far, which is about 140 figures in decimal. Consequently, attacks using these methods are not threatening in practice if n is 1024 bits or so.

[0016] In addition, there are cases where a public key cryptosystem apparatus can be used as an authentication apparatus by reversing the public key and secret key calculations in general.

SUMMARY OF THE INVENTION

[0017] It is therefore an object of the present invention to provide a new scheme for encryption, decryption and authentication which is capable of overcoming the problems associated with the conventionally known RSA cryptosystem as described above.

[0018] More specifically, objects of the present invention are:

(1) to realize an encryption/decryption scheme which has the same security level compared with the known RSA cryptosystem on rational integer ring,

(2) to realize an encryption/decryption scheme for which the encryption/decryption processing is faster than the conventional RSA cryptosystem,

(3) to realize an encryption/decryption scheme which can also be utilized as an authentication scheme such that a single apparatus can be used for both the cipher communications and the authentication, and

(4) to realize an authentication scheme for which the authenticator generation and the verification are faster than the known authentication scheme based on the conventional RSA cryptosystem.

[0019] According to one aspect of the present invention there is provided an encryption method, comprising the steps of: setting N (≥ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$ as a first secret key, and a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ as a first public key n, where k1, k2, $\cdots\cdots\cdots$, kN are arbitrary positive integers; determining a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of $p_1-1, p_2-1, \cdots\cdots\cdots, p_N-1$, using the first secret key; and obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e.

[0020] According to another aspect of the present invention there is provided a decryption method for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^{e} \pmod{n}$$

using a first secret key given by N (≧ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ·····, p_N-1, the method comprising the steps of: obtaining residues $M_{p1k1}, M_{p2k2}, \cdots\cdots\cdots, M_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, \cdots\cdots\cdots, p_N^{kN}$, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key $p_1, p_2, \cdots\cdots\cdots, p_N$; and recovering the plaintext M by applying Chinese remainder theorem to the residues $M_{p1k1}, M_{p2k2}, \cdots\cdots\cdots, M_{pNkN}$.

[0021] According to another aspect of the present invention there is provided an authentication method for authenticating an authentication message sent from a sender to a receiver, comprising the steps of: (a) setting at the sender side a first secret key given by N (≧ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ·····, p_N-1; (b) obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; (c) obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^{e} \pmod{n}$$

by obtaining residues $h(C)_{p1k1}, h(C)_{p2k2}, \cdots\cdots\cdots, h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, \cdots\cdots\cdots, p_N^{kN}$, respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first secret key $p_1, p_2, \cdots\cdots\cdots, p_N$, and applying Chinese remainder theorem to the residues $h(C)_{p1k1}, h(C)_{p2k2}, \cdots\cdots\cdots, h(C)_{pNkN}$; (d) sending the encrypted authenticator h(C) and the authentication message M from the sender to the receiver; (e) obtaining at the receiver side a first authenticator $h(M)_1$ by calculating $h(C)^e \pmod{n}$ from the encrypted authenticator h(C) received from the sender using the second public key e; (f) obtaining at the receiver side a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h; and (g) judging an authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0022] According to another aspect of the present invention there is provided an encryption apparatus, comprising: an encryption/decryption key generation processing unit for setting N (≧ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$ as a first secret key, and a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ as a first public key n, where k1, k2, ·····, kN are arbitrary positive integers, and determining a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ·····, p_N-1, using the first secret key; and an encryption processing unit for obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^{e} \pmod{n}$$

using the first public key n and the second public key e.

[0023] According to another aspect of the present invention there is provided a decryption apparatus for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^{e} \pmod{n}$$

using a first secret key given by N (≧ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, ·····, kN are arbitrary positive integers, a second public key e

and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・, p_N-1, the apparatus comprising: a calculation processing unit for obtaining residues $M_{p\,1\,k\,1}$, $M_{p\,2\,k\,2}$, ・・・・・・・・, $M_{p\,N\,k\,N}$ modulo $p_1^{\,k\,1}$, $p_2^{\,k\,2}$, ・・・・・・・・, $p_N^{\,k\,N}$, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key p_1, p_2, ・・・・・・・・, p_N; and a decryption processing unit for recovering the plaintext M by applying Chinese remainder theorem to the residues $M_{p\,1\,k\,1}$, $M_{p\,2\,k\,2}$, ・・・・・・・・, $M_{p\,N\,k\,N}$.

[0024] According to another aspect of the present invention there is provided a cipher communication system, comprising: a sender apparatus having: an encryption/decryption key generation processing unit for setting N (≧ 2) prime numbers p_1, p_2, ・・・・・・・・, p_N as a first secret key, and a product $p_1^{\,k\,1}\,p_2^{\,k\,2}$ ・・・・・・・・ $p_N^{\,k\,N}$ as a first public key n, where k1, k2, ・・・・・・・・, kN are arbitrary positive integers, and determining a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・, p_N-1, using the first secret key; and an encryption processing unit for obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e; and a receiver apparatus having: a calculation processing unit for obtaining residues $M_{p\,1\,k\,1}$, $M_{p\,2\,k\,2}$, ・・・・・・・・, $M_{p\,N\,k\,N}$ modulo $p_1^{\,k\,1}$, $p_2^{\,k\,2}$, ・・・・・・・・, $p_N^{\,k\,N}$, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key p_1, p_2, ・・・・・・・・, p_N; and a decryption processing unit for recovering the plaintext M by applying Chinese remainder theorem to the residues $M_{p\,1\,k\,1}$, $M_{p\,2\,k\,2}$, ・・・・・・・・, $M_{p\,N\,k\,N}$.

[0025] According to another aspect of the present invention there is provided an authentication message sender apparatus for use in authenticating an authentication message sent from a sender to a receiver, the apparatus comprising: an encryption/decryption key generation processing unit for setting at the sender side a first secret key given by N (≧ 2) prime numbers p_1, p_2, ・・・・・・・・, p_N, a first public key n given by a product $p_1^{\,k\,1}\,p_2^{\,k\,2}$ ・・・・・・・・ $p_N^{\,k\,N}$ where k1, k2, ・・・・・・・・, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・, p_N-1; an authentication message hashing processing unit for obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and an authenticator encryption processing unit for obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p\,1\,k\,1}$, $h(C)_{p\,2\,k\,2}$, ・・・・・・・・, $h(C)_{p\,N\,k\,N}$ modulo $p_1^{\,k\,1}$, $p_2^{\,k\,2}$, ・・・・・・・・, $p_N^{\,k\,N}$, respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first secret key p_1, p_2, ・・・・・・・・, p_N, and applying Chinese remainder theorem to the residues $h(C)_{p\,1\,k\,1}$, $h(C)_{p\,2\,k\,2}$, ・・・・・・・・, $h(C)_{p\,N\,k\,N}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver.

[0026] According to another aspect of the present invention there is provided an authentication message receiver apparatus for use in authenticating an authentication message sent from a sender to a receiver, using a first secret key given by N (≧ 2) prime numbers p_1, p_2, ・・・・・・・・, p_N, a first public key n given by a product $p_1^{\,k\,1}\,p_2^{\,k\,2}$ ・・・・・・・・ $p_N^{\,k\,N}$ where k1, k2, ・・・・・・・・, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・, p_N-1, the apparatus comprising: an authenticator decryption processing unit for obtaining a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from an encrypted

authenticator h(C) received from the sender using the second public key e; an authentication message hashing processing unit for obtaining a second authenticator $h(M)_2$ by hashing an authentication message M received from the sender using a hash function h; and an authenticity verification processing unit for judging an authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0027] According to another aspect of the present invention there is provided an authentication system for authenticating an authentication message sent from a sender to a receiver, the system comprising: a sender apparatus having: an encryption/decryption key generation processing unit for setting at the sender side a first secret key given by N (≥ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, $\cdots\cdots\cdots$, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of $p_1-1, p_2-1, \cdots\cdots\cdots, p_N-1$; an authentication message hashing processing unit for obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and an authenticator encryption processing unit for obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) = h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}, h(C)_{p2k2}, \cdots\cdots\cdots, h(C)_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, \cdots\cdots\cdots, p_N^{kN}$, respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first secret key $p_1, p_2, \cdots\cdots\cdots, p_N$, and applying Chinese remainder theorem to the residues $h(C)_{p1k1}, h(C)_{p2k2}, \cdots\cdots\cdots, h(C)_{pNkN}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver; and a receiver apparatus having: an authenticator decryption processing unit for obtaining a first authenticator $h(M)_1$ by calculating $h(C)^e \pmod{n}$ from the encrypted authenticator h(C) received from the sender using the second public key e; an authentication message hashing processing unit for obtaining a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h; and an authenticity verification processing unit for judging an authenticity of the authentication message M by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0028] According to another aspect of the present invention there is provided a computer usable medium having computer readable program code means embodied therein for causing a computer to function as an encryption apparatus, the computer readable program code means includes: first computer readable program code means for causing said computer to set N (≥ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$ as a first secret key, and a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ as a first public key n, where k1, k2, $\cdots\cdots\cdots$, kN are arbitrary positive integers, and determining a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of $p_1-1, p_2-1, \cdots\cdots\cdots, p_N-1$, using the first secret key; and second computer readable program code means for causing said computer to obtain a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e.

[0029] According to another aspect of the present invention there is provided a computer usable medium having computer readable program code means embodied therein for causing a computer to function as a decryption apparatus for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using a first secret key given by N (≥ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, $\cdots\cdots\cdots$, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of $p_1-1, p_2-1, \cdots\cdots\cdots, p_N-1$, the computer readable program code means

includes: first computer readable program code means for causing said computer to obtain residues $M_{p\,1\,k\,1}$, $M_{p\,2\,k\,2}$, ·····, $M_{p\,N\,k\,N}$ modulo $p_1^{k\,1}$, $p_2^{k\,2}$, ·····, $p_N^{k\,N}$, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key p_1, p_2, ·····, p_N; and second computer readable program code means for causing said computer to recover the plaintext M by applying Chinese remainder theorem to the residues $M_{p\,1\,k\,1}$, $M_{p\,2\,k\,2}$, ·····, $M_{p\,N\,k\,N}$.

[0030] According to another aspect of the present invention there is provided a computer usable medium having computer readable program code means embodied therein for causing a computer to function as an authentication message sender apparatus for use in authenticating an authentication message sent from a sender to a receiver, the computer readable program code means includes: first computer readable program code means for causing said computer to set at the sender side a first secret key given by N (≧ 2) prime numbers p_1, p_2, ·····, p_N, a first public key n given by a product $p_1^{k\,1}\,p_2^{k\,2}$ ····· $p_N^{k\,N}$ where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ·····, p_N-1; second computer readable program code means for causing said computer to obtain at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and third computer readable program code means for causing said computer to obtain at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p\,1\,k\,1}$, $h(C)_{p\,2\,k\,2}$, ·····, $h(C)_{p\,N\,k\,N}$ modulo $p_1^{k\,1}$, $p_2^{k\,2}$, ·····, $p_N^{k\,N}$, respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first secret key p_1, p_2, ·····, p_N, and applying Chinese remainder theorem to the residues $h(C)_{p\,1\,k\,1}$, $h(C)_{p\,2\,k\,2}$, ·····, $h(C)_{p\,N\,k\,N}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver.

[0031] According to another aspect of the present invention there is provided a computer usable medium having computer readable program code means embodied therein for causing a computer to function as an authentication message receiver apparatus for use in authenticating an authentication message sent from a sender to a receiver, using a first secret key given by N (≧ 2) prime numbers p_1, p_2, ·····, p_N, a first public key n given by a product $p_1^{k\,1}\,p_2^{k\,2}$ ····· $p_N^{k\,N}$ where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ·····, p_N-1, the computer readable program code means includes: first computer readable program code means for causing said computer to obtain a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from an encrypted authenticator h(C) received from the sender using the second public key e; second computer readable program code means for causing said computer to obtain a second authenticator $h(M)_2$ by hashing an authentication message M received from the sender using a hash function h; and third computer readable program code means for causing said computer to judge an authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0032] Other features and advantages of the present invention will become apparent from the following description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033]

Fig. 1 is a block diagram of a cipher communication system according to one embodiment of the present invention.

Fig. 2 is a flow chart for an encryption processing of an encryption apparatus in the cipher communication system of Fig. 1.

Fig. 3 is a flow chart for a decryption processing of a decryption apparatus in the cipher communication system of Fig. 1.

Fig. 4 is a block diagram of an authentication system according to one embodiment of the present invention.

Fig. 5 is a flow chart for an authentication processing in the authentication system of Fig. 4.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0034] Referring now to Fig. 1 to Fig. 4, one embodiment of the scheme for encryption, decryption and authentication according to the present invention will be described in detail.

[0035] Note that the encryption/decryption scheme of the present invention is realizable using $n = p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ in general, as will be described below, but the more practical exemplary case of using $n = p_1^{k1} p_2$ will be described first. In the following, an expression "$p^k q$" corresponds to a special case of the general expression $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ (where $p_1, p_2, \cdots\cdots\cdots, p_N$ are ($\geqq 2$) prime numbers) with $N = 2$, $p_1 = p$, $p_2 = q$, $k1 = k$ and $k2 = 1$.

[0036] Fig. 1 shows an overall configuration of a cipher communication system according to one embodiment of the present invention.

[0037] The cipher communication system of Fig. 1 generally comprises an encryption apparatus 10 and a decryption apparatus 19 which are connected through a communication path 14. The encryption apparatus 10 has an encryption processing unit 13 for obtaining a ciphertext C from a plaintext M given as its input, and transmitting the obtained ciphertext C to the decryption apparatus 19 through the communication path 14. The decryption apparatus 19 has a decryption processing unit 15 for recovering the plaintext M from the ciphertext C transmitted by the encryption processing unit 13, and outputting the obtained plaintext M as its output. This decryption processing unit 15 includes a loop calculation processing unit 17.

[0038] In addition, the encryption apparatus 10 also has an encryption/decryption key generation processing unit 11 connected with both the encryption processing unit 13 and the decryption processing unit 15, for supplying the first public key n and the second public key e to the encryption processing unit 13 while supplying the first secret key p, q, the second secret key d, an arbitrary positive integer k, the first public key n and the second public key e to the decryption processing unit 15.

[0039] Next, the operation of the encryption apparatus 10 will be described in detail with reference to Fig. 2.

[0040] First, the encryption/decryption keys are generated at the encryption/decryption key generation processing unit 11 as follows (step S101).

[0041] Here, the first secret key is to be given by two rational prime numbers p and q, and the first public key is to be given by their product, i.e., $n = p^k q$. Also, using the function lcm for obtaining the least common multiple, L given by:

$$L = \mathrm{lcm}\,(p-1, q-1)$$

is obtained from the first secret key p and q.

[0042] Next, e and d that satisfies:

$$ed \equiv 1 \pmod{L}$$

are obtained. Then, the residues d_p and d_q of the obtained d modulo (p-1) and (q-1) respectively are obtained as:

$$d_p := d \pmod{p-1},$$

$$d_q := d \pmod{q-1},$$

where a symbol ":=" denotes the operation to calculate the right hand side and substitute it into the left hand side, and a set of three numbers d, dp and dq is set as the second secret key, while e is set as the second public key. In this way, the first public key n, the second public key e, the first secret key p, q, and the second secret key d, d_p and d_q are set up.

[0043] Then, the ciphertext C is obtained at the encryption processing unit 13 as follows (step S102).

[0044] The encryption processing unit 13 encrypts the plaintext M by using the first public key n and the second public key e, according to the formula:

$$C \equiv M^e \pmod{n}$$

and transmits the obtained ciphertext C to the receiving side.

[0045] Next, the operation of the decryption apparatus 19 will be described in detail with reference to Fig. 3.

[0046] The decryption processing unit 15 obtains the plaintext M as an output from the ciphertext C entered from the encryption processing unit 13 through the communication path, the first secret key p, q, the second secret key d, the second public key e and the arbitrary positive integer k which are entered from the encryption/decryption key generation processing unit 11, by carrying out the following substitution calculation processing, where a symbol ":=" denotes the operation to calculate the right hand side and substitute it into the left hand side.

[0047] (Step S201) The values d_p and d_q of the second secret key d modulo p-1 and q-1 respectively are obtained as follows.

$$d_p := d \pmod{p-1},$$

$$d_q := d \pmod{q-1}.$$

Note that there is no need to calculate these d (mod p-1) and d (mod q-1) at every occasion of the encryption/decryption and it suffices to produce them once in advance as the secret key. In such a case, d will be necessary only at the intermediate stage for producing these d (mod p-1) and d (mod q-1).

[0048] (Step S202) The residues $K_\emptyset$, M_q of the plaintext M modulo p and q respectively are obtained from the ciphertext C as follows.

$$K_\emptyset := C^{d_p} \pmod{p},$$

$$M_q := C^{d_q} \pmod{q}.$$

[0049] (Step S203) The residue M_{p^k} of the plaintext M modulo p^k is obtained by carrying out the following loop calculation according to the fast decryption algorithm disclosed in T. Takagi, "Fast RSA-type cryptosystem using n-adic expansion", Advances in Cryptology - CRYPTO'97, LNCS 1294, pp. 372-384 and in U.S. Patent Application Serial No. 08/907,852 of the present inventors, at the loop calculation processing unit 17.

$A_0 := K_0$;
FOR i = 1 to (k-1) do
begin
$F_i := (A_{i-1}^e) \pmod{p^{i+1}}$;
$E_i := (C - F_i) \pmod{p^{i+1}}$;
$B_i := E_i / p^i$ in Z;
$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p}$;
$A_i := A_{i-1} + p^i K_i$ in Z;
end
$M_{p^k} := A_{k-1}$.

[0050] (Step S204) The residue of the plaintext M with respect to a composite number n is obtained by applying the Chinese remainder theorem to the residues M_{p^k} and M_q , so as to complete the decryption.

[0051] More specifically, the Chinese remainder theorem can be applied by the following calculation.

$$q_1 := q^{-1} \pmod{p^k};$$

$$v_1 := ((M_{p^k} - M_q) q_1) \pmod{p^k};$$

$$M := (M_q + q v_1).$$

Alternatively, the Chinese remainder theorem can also be applied by the following calculation.

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$v_1 := ((M_q - M_{p^k}) p_1) \pmod{q};$$

$$M := (M_{p^k} + p^k v_1).$$

Alternatively, the Chinese remainder theorem can also be applied by the following calculation.

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$q_1 := q^{-1} \pmod{p^k};$$

$$M := (q_1 q M_{pk} + p_1 p^k M_q) \pmod{p^k q}.$$

[0052] Next, the functions of the respective processing units in the cipher communication system of Fig. 1 will be described along their processing procedure.

[0053] First, as the first stage, at the encryption/decryption key generation processing unit 11, two prime numbers p and q to be the first secret key are generated, and the product $n = p^k q$ of these two prime numbers p and q is obtained as the first public key. Here, k is an arbitrary integer to be selected by accounting for the security level and the processing speed. Also, as can be seen from the formula $n = p^k q$ for the first public key n, the sizes of p and q can be made smaller when k is larger for a constant size (the number of digits, for example) of n, and the prime factoring becomes as much easier (that is, it becomes easier to learn the values of p and q) so that the security level of this cryptosystem becomes lower.

[0054] Next, the least common multiple L is calculated from these two prime numbers p and q, and the second pubic key e and the second secret key d are generated according to $ed \equiv 1 \pmod{L}$. This calculation of the least common multiple L can be done by first obtaining the greatest common divisor using the extended Euclidean division algorithm and then multiplying the remaining factors to obtain the least common multiple.

[0055] Note that the pair of e and d at this point is uniquely determined from $ed \equiv 1 \pmod{L}$. Although it can be any pair that satisfies this condition in principle, usually the second public key e is set to be a smaller value in order to make the encryption faster. For this reason, the second secret key d becomes a considerably large number so that the decryption processing becomes slow when the conventional scheme is adopted. Note that the second public key e and the second secret key d are in relationship of inverse numbers modulo L, so that the second secret key d can be obtained if the second public key e and the least common multiple L are known.

[0056] Next, as the second stage, at the encryption processing unit 13, the encryption is carried out according to the formula:

$$C \equiv M^e \pmod{n}$$

using the second public key e of the receiving side, and the ciphertext C is transmitted to the receiving side.

[0057] Then, as the third stage, at the decryption processing unit 15, $M_{pk} \equiv M \pmod{p^k}$ and $M_q \equiv C^{dq} \pmod{q}$ are obtained using the aforementioned fast decryption algorithm, and the Chinese remainder theorem is applied to these two numbers. According to the Chinese remainder theorem, when the residues of an unknown number for plural moduli are known, the unknown number (solution) modulo a product of these plural moduli can be obtained uniquely so that M can be recovered.

[0058] Now, concrete examples of the encryption according to this embodiment will be described.

[0059] First, the exemplary case of k = 2 can be summarized as follows.

Public key e = 5
Public key n = 40270132689707
Secret key d = 234982541
Secret key p = 34273
Secret key q = 34283
Plaintext M = 1234567890
Ciphertext C = 10229049760163
$A_\phi = K_\phi = 20157$
$M_q = 2777$
$K_1 = 1748$
$M_p = A_\phi + pK_1 = 59929361$
Plaintext M = 1234567890

[0060] In this case, the value of each one of the first secret key p and q is about $n^{1/(k+1)}$, and the least common multiple L is about $n^{2/(k+1)}$ which is smaller than the RSA cryptosystem so that it can contribute to the realization of the faster encryption/decryption.

[0061] More specifically, the calculation time for $C^d \bmod n$ is $0((\log n)^2(\log d))$ while the calculation time for $C^d \bmod p$

and C^d mod q is $0(1/3 \log n)^2(2/3 \log n)$. Thus the overall processing time is 0.148 times that of the RSA cryptosystem, and it is a little over three times faster than the Quisquater-Couvreur scheme that utilizes the Chinese remainder theorem (which has the calculation time of $0(1/2 \log n)^2(1 \log n)$).

[0062] Next, the exemplary case of k = 3 can be summarized as follows.

Public key e = 5
Public key n = 627252701350243
Secret key d = 7515005
Secret key p = 5003
Secret key q = 5009
Plaintext M = 123456789012345
Ciphertext C = 287551735059915
$A_\phi = K_{\phi p} = 1732$
$M_q = 3412$
$K_{1p} = 4821$
$A_1 = 24121195$
$K_{2p} = 4395$
$M_{p2} = A_2 = A_1 + p^2K_2 = 110031010750$
Plaintext M = 123456789012345

[0063] It should be apparent that the encryption/decryption scheme described above is also applicable to the case of using three prime numbers $p_1 = p$, $p_2 = q$ and $p_3 = r$ as the first secret key and a product $p^k q^\ell r^m$ where $k = k1$, $\ell = k2$ and $m = k3$ as the first public key n.

[0064] In this case, the decryption can be realized by first obtaining $K_\phi{}^p$, $K_\phi{}^q$ and $K_\phi{}^r$ modulo p, q and r, respectively, by integer modular exponent calculations of:

$$K_\phi{}^p := C^{dp} \pmod p;$$

$$K_\phi{}^q := C^{dq} \pmod q;$$

$$K_\phi{}^r := C^{dr} \pmod r;$$

where:

$$dp := d \pmod{p-1};$$

$$dq := d \pmod{q-1};$$

$$dr := d \pmod{r-1};$$

next obtaining the residues M_{pk}, $M_{q\ell}$ and M_{rm} modulo p^k, q^ℓ and r^m, respectively, by applying the loop calculation to $K_\phi{}^p$, $K_\phi{}^q$ and $K_\phi{}^r$, respectively, and then applying the Chinese remainder theorem to the residues M_{pk}, $M_{q\ell}$ and M_{rm}.

[0065] It should also be apparent that the encryption/decryption scheme described above can be generalized to the case of using N (≧ 2) prime numbers p_1, p_2, ・・・・・・・・, p_N as a first secret key, and a product $p_1{}^{k1}\ p_2{}^{k2}$ ・・・・・・・・ $p_N{}^{kN}$ as a first public key n, where k1, k2, ・・・・・・・・, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed = 1 \pmod L$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・, P_N-1.

[0066] In this general case, a ciphertext C can be obtained from a plaintext M according to:

$$C \equiv M^e \pmod n$$

using the first public key n and the second public key e defined above.

[0067] Also in this case, the decryption can be realized by first obtaining residues M_{p1k1}, M_{p2k2}, ・・・・・・・・, M_{pNkN} modulo $p_1{}^{k1}$, $p_2{}^{k2}$, ・・・・・・・・, $p_N{}^{kN}$, respectively, of the plaintext M using the loop calculation of the

aforementioned fast decryption algorithm with respect to the first secret key p_1, p_2, ・・・・・・・・, p_N, and then applying the Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ・・・・・・・・, M_{pNkN}.

[0068] Next, Fig. 4 shows an overall configuration of an authentication system according to one embodiment of the present invention.

[0069] The authentication system of Fig. 4 generally comprises a sender apparatus 20 and a receiver apparatus 33 which are connected through a communication path 26. The sender apparatus 20 has an authentication message hashing processing unit 23 for outputting an authenticator h(M) by applying a hashing processing on an input authentication message (plaintext) M, and an authenticator encryption processing unit 25 for encrypting the authenticator h(M) outputted from the authentication message hashing processing unit 23 and transmitting the obtained encrypted authenticator h(C) through a communication path 26.

[0070] The receiver apparatus 33 has an authenticator decryption processing unit 27 for obtaining a first authenticator $h(M)_1$ from the encrypted authenticator h(C) and an authentication message hashing processing unit 29 for obtaining a second authenticator $h(M)_2$ from the authentication message M, both of which are connected to the authentication encryption processing unit 25 through the communication path 26, and an authenticity verification processing unit 31 for verifying an authenticity of the authentication message M, which is connected with the authenticator decryption processing unit 27 and the authentication message hashing processing unit 29.

[0071] In addition, the sender apparatus 20 also has an authentication encryption/decryption key generation processing unit 21 for outputting authentication encryption/decryption keys to the authenticator encryption processing unit 25 and the authenticator decryption processing unit 27 respectively.

[0072] This authentication system of Fig. 4 realizes the authentication scheme in which a person who wishes to have the own authentication message authenticated will send to the receiving side an authenticator generated by encrypting the authentication message by using the own secret key.

[0073] Now, the operations of the respective processing units in the authentication system of Fig. 4 will be described along their processing procedure with reference to Fig. 5.

[0074] First, as the first stage (step S301), at the authentication encryption/decryption key generation processing unit 21, two prime numbers p and q to be the first secret key are generated, and the product $n = p^k q$ of these two prime numbers p and q is obtained as the first public key. Here, k is an arbitrary integer to be selected by accounting for the security level and the processing speed. Also, as can be seen from the formula $n = p^k q$ for the first public key n, the sizes of p and q can be made smaller when k is larger for a constant size (the number of digits, for example) of n, and the prime factoring becomes as much easier (that is, it becomes easier to learn the values of p and q) so that the security level of this cryptosystem becomes lower. Then, the least common multiple L is calculated from these two prime numbers p and q, and the second pubic key e and the second secret key d are generated according to $ed \equiv 1 \pmod{L}$.

[0075] Next, as the second stage (step S302), at the authentication message hashing processing unit 23, the plaintext authentication message M is hashed by using the hash function h to obtain the authenticator h(M), where it is assumed that $0 \leqq h(M) < n$. Here, the hash function is used in order to shorten the message length. For example, the hashing processing extracts several characters from the top of the message. Also, a certain level of the scrambling function is to be provided. Note that the same hash function is to be used at the sending side and the receiving side.

[0076] Next, as the third stage (step S303), at the authenticator encryption processing unit 25, the encrypted authenticator h(C) is calculated by the technique of the aforementioned fast decryption algorithm, using the first public key n and the second secret key d of the sending side. Note that, in the authentication, the decryption processing and the encryption processing become completely reversed from the case of the encryption/decryption scheme described above, so that the calculation of the encrypted authenticator h(C) can be processed quickly by using the Chinese remainder theorem.

[0077] After this calculation processing, the set of the encrypted authenticator h(C) and the authentication message M is transmitted to the receiving side through the communication path.

[0078] Next, as the fourth stage (step S304), at the authenticator decryption processing unit 27, the receiving side decrypts the encrypted authenticator h(C) by calculating:

$$h(M)_1 = h(C)^e \pmod{n}$$

using the second public key e of the sending side, so as to obtain the first authenticator $h(M)_1$.

[0079] Next, as the fifth stage (step S305), at the authentication message hashing processing unit 29, the receiving side hashes the authentication message M by using the hash function h so as to obtain the second authenticator $h(M)_2$.

[0080] Then, as the sixth stage (step S306), at the authenticity verification processing unit 31, the authenticity of the authentication message is judged according to whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide with each other or not, and an output indicating either coincide (Yes) or not coincide (No) is outputted.

[0081] More specifically, the authentication scheme according to the present invention can be realized as follows.

[0082] In the most general case, the sender side sets a first secret key given by N (≧ 2) prime numbers p_1, p_2,

$\cdots\cdots\cdots$, p_N, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, $\cdots\cdots\cdots$, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, $\cdots\cdots\cdots$, p_N-1.

[0083] Then, the sender side obtains an authenticator h(M) by hashing the authentication message M using a hash function h, while obtaining an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, $\cdots\cdots\cdots$, $h(C)_{pNkN}$ modulo p_1^{k1}, p_2^{k2}, $\cdots\cdots\cdots$, p_N^{kN}, respectively, of the encrypted authenticator h(C) using the loop calculation of the aforementioned fast decryption algorithm with respect to the first secret key p_1, p_2, $\cdots\cdots\cdots$, p_N, and applying the Chinese remainder theorem to the residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, $\cdots\cdots\cdots$, $h(C)_{pNkN}$.

[0084] Then, the encrypted authenticator h(C) and the authentication message M are sent from the sender to the receiver.

[0085] Next, the receiver side obtains a first authenticator $h(M)_1$ by calculating $h(C)^e \pmod{n}$ from the encrypted authenticator h(C) received from the sender using the second public key e, while obtaining a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h.

[0086] Then, an authenticity of the authentication message M is judged at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

[0087] It should be apparent from the above that, in the specific case where the encrypted authenticator h(C) is obtained using the first secret key given by three prime numbers $p_1 = p$, $p_2 = q$ and $p_3 = r$ and the first public key n given by a product $p^k q^\ell r^m$ where $k = k1$, $\ell = k2$ and $m = k3$, the sender obtains the encrypted authenticator h(C) by first obtaining $h(K)_\emptyset^{\,p}$, $h(K)_\emptyset^{\,q}$ and $h(K)_\emptyset^{\,r}$ modulo p, q and r, respectively, by integer modular exponent calculations of:

$$h(K)_\emptyset^{\,p} := h(M)^{dp} \pmod{p};$$

$$h(H)_\emptyset^{\,q} := h(M)^{dq} \pmod{q};$$

$$h(K)_\emptyset^{\,r} := h(M)^{dr} \pmod{r};$$

where:

$$dp := d \pmod{p-1};$$

$$dq := d \pmod{q-1};$$

$$dr := d \pmod{r-1};$$

next obtaining the residues $h(C)_{pk}$, $h(C)_{q\ell}$ and $h(C)_{rm}$ modulo p^k, q^ℓ and r^m, respectively, by applying the loop calculation to $h(K)_\emptyset^{\,p}$, $h(K)_\emptyset^{\,q}$ and $h(K)_\emptyset^{\,r}$, respectively, and then applying the Chinese remainder theorem to the residues $h(C)_{pk}$, $h(C)_{q\ell}$ and $h(C)_{rm}$.

[0088] It should also be apparent from the above that, in the specific case where the encrypted authenticator h(C) is obtained using the first secret key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by a product $p^k q$ where $k = k1$, the sender obtains the encrypted authenticator h(C) by first obtaining a residue $h(K)_\emptyset$ modulo p and a residue $h(C)_q$ modulo q of the encrypted authenticator h(C), by integer modular exponent calculations of:

$$h(K)_\emptyset := h(M)^{dp} \pmod{p};$$

$$h(C)_q := h(M)^{dq} \pmod{q};$$

where:

$$dp := d \pmod{p-1};$$

$$dq := d \pmod{q-1};$$

next obtaining a residue $h(C)_{pk}$ modulo p^k of the encrypted authenticator h(C) by applying the loop calculation to $h(K)_0$, and then applying the Chinese remainder theorem to the residues $h(C)_{pk}$ and $h(C)_q$.

[0089] In this case, the loop calculation can be carried out as follows.

```
h(A)0  := h(K)0 ;
FOR i = 1 to (k-1) do
begin
h(F)i  := (h(A)i-1^e) (mod p^(i+1));
h(E)i  := (h(M) - h(F)i) (mod p^(i+1));
h(B)i  := h(E)i/p^i in Z;
h(K)i  := ((eh(F)i)^-1 h(A)i-1 h(B)i) (mod p);
h(A)i  := h(A)i-1 + p^i h(K)i in Z;
end
h(C)pk  := h(A)k-1 .
```

[0090] Also in this case, the Chinese remainder theorem can be applied by the following calculation.

$$q_1 := q^{-1} \pmod{p^k};$$

$$v_1 := ((h(C)_{pk} - h(C)_q)q_1) \pmod{p^k};$$

$$h(C) := (h(C)_q + qv_1).$$

Alternatively, the Chinese remainder theorem can also be applied by the following calculation.

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$v_1 := ((h(C)_q - h(C)_{pk})p_1) \pmod{q};$$

$$h(C) := (h(C)_{pk} + p^k v_1).$$

Alternatively, the Chinese remainder theorem can also be applied by the following calculation.

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$q_1 := q^{-1} \pmod{p^k};$$

$$h(C) := (q_1 qh(C)_{pk} + p_1 p^k h(C)_q) \pmod{p^k q}.$$

[0091] Note that, in the above described embodiment, each of the prime numbers has a size of about $n^{1/(k+1)}$ which is sufficient to prevent the number field sieve method and the elliptic curve method that are the fastest prime factoring algorithms currently known. Also, the second public key e can be set small so that the second secret key d has about the same size as the least common multiple L. Here, the least common multiple L has a size of $n^{2/(k+1)}$ which is smaller than that of the RSA cryptosystem so that it can contribute to the realization of the faster encryption/decryption.

[0092] Also, in the above described embodiment, the case of k = 3 uses the composite number $n = p^3q$ as the modulus, so that the size of each of p and q becomes 1/4 of the size of n. The decryption processing modulo p^3 requires about the same amount of calculations as the processing modulo p, so that the processing modulo p^3 and the processing modulo q can be made 64 times faster. Thus the overall processing can be made 32 times faster, which is considerably faster even in comparison with the conventional Quisquater-Couvreur scheme that can realize four times faster decryption processing than the original RSA cryptosystem.

[0093] As described, the cryptosystem according to the present invention uses N (≧ 2) prime numbers p_1, p_2,

$\cdots\cdots\cdots$, p_N as the first secret key and their product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ as the first public key n, so that it has the same security level as the conventionally known RSA cryptosystem on rational integer ring, while it is capable of realizing the faster encryption and decryption processing. In addition, it can be utilized for the authentication as well, and it is also capable of realizing the faster authenticator generation and authenticity verification.

[0094] Moreover, the cryptosystem according to the present invention uses the second public key e as an encryption key and the second secret key d as a decryption key which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, $\cdots\cdots\cdots$, p_N-1, so that the size of the decryption key d can be made about the same as the size of L.

[0095] In contrast, in the case of the RSA cryptosystem for example, if $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ is to be used as the first public key n where p_1, p_2, $\cdots\cdots\cdots$, p_N are N ($\geq$ 2) prime numbers, it is required to generate the encryption key e and the decryption key d which satisfy:

$$ed \equiv 1 \pmod{\phi(n)}$$

where

$$\phi(n) = n(1-1/p_1)(1-1/p_2) \cdots\cdots\cdots (1-1/p_N)$$

is the Euler function, so that the size of the decryption key d becomes the same as the size of $\phi(n)$ which is considerably larger than the size of L.

[0096] It is to be noted that the above described embodiment according to the present invention may be conveniently implemented in forms of software programs for realizing the operations of the cipher communication system of Fig. 1 or the authentication system of Fig. 4, as will be apparent to those skilled in the computer art. Appropriate software coding can readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art.

[0097] In particular, each of the encryption apparatus and the decryption apparatus of Fig. 1 and the sender apparatus and the receiver apparatus of Fig. 4 as described above can be conveniently implemented in a form of a software package.

[0098] Such a software package can be provided in a form of a computer program product which employs a storage medium including stored computer code which is used to program a computer to perform the disclosed function and process of the present invention. The storage medium may include, but is not limited to, any type of conventional floppy disks, optical disks, CD-ROMs, magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, or any other suitable media for storing electronic instructions.

[0099] It is also to be noted that, besides those already mentioned above, many modifications and variations of the above embodiments may be made without departing from the novel and advantageous features of the present invention. Accordingly, all such modifications and variations are intended to be included within the scope of the appended claims.

Claims

1. An encryption method, comprising the steps of:

setting N ($\geq$ 2) prime numbers p_1, p_2, $\cdots\cdots\cdots$, p_N as a first secret key, and a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ as a first public key n, where k1, k2, $\cdots\cdots\cdots$, kN are arbitrary positive integers;

determining a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, $\cdots\cdots\cdots$, p_N-1, using the first secret key; and

obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e.

2. The method of claim 1, wherein the setting step sets three prime numbers $p_1 = p$, $p_2 = q$ and $p_3 = r$ as the first secret key and a product $p^k q^\ell r^m$ where k = k1, ℓ = k2 and m = k3 as the first public key n.

3. The method of claim 1, wherein the setting step sets two prime numbers $p_1 = p$ and $p_2 = q$ as the first secret key and a product $p^k q$ where k = k1 as the first public key n.

4. The method of claim 3, wherein the determining step also determines:

$$d_p := d \pmod{p-1}, \text{ and}$$

$$d_q := d \pmod{q-1},$$

as the second secret key such that the second secret key is given by a set of d, d_p and d_q.

5. A decryption method for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using a first secret key given by N (≧ 2) prime numbers $p_1, p_2, \cdots\cdots\cdots, p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of $p_1-1, p_2-1, \cdots\cdots\cdots, p_N-1$, the method comprising the steps of:

obtaining residues $M_{p\,1\,k\,1}, M_{p\,2\,k\,2}, \cdots\cdots\cdots, M_{p\,N\,k\,N}$ modulo $p_1^{k1}, p_2^{k2}, \cdots\cdots\cdots, p_N^{kN}$, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key $p_1, p_2, \cdots\cdots\cdots, p_N$; and

recovering the plaintext M by applying Chinese remainder theorem to the residues $M_{p\,1\,k\,1}, M_{p\,2\,k\,2}, \cdots\cdots\cdots, M_{p\,N\,k\,N}$.

6. The method of claim 5, wherein the ciphertext C is obtained using the first secret key given by three prime numbers $p_1 = p$, $p_2 = q$ and $p_3 = r$ and the first public key n given by a product $p^k q^\ell r^m$ where k = k1, ℓ = k2 and m = k3;

the obtaining step obtains $K_\phi{}^p$, $K_\phi{}^q$ and $K_\phi{}^r$ modulo p, q and r, respectively, by integer modular exponent calculations of:

$$K_\phi{}^p := C^{dp} \pmod{p};$$

$$K_\phi{}^q := C^{dq} \pmod{q}; \text{ and}$$

$$K_\phi{}^r := C^{dr} \pmod{r};$$

where:

$$dp := d \pmod{p-1};$$

$$dq := d \pmod{q-1}; \text{ and}$$

$$dr := d \pmod{r-1};$$

and then obtaining the residues $M_{p\,k}$, $M_{q\,\ell}$ and $M_{r\,m}$ modulo p^k, q^ℓ and r^m, respectively, by applying the prescribed loop calculation to $K_\phi{}^p$, $K_\phi{}^q$ and $K_\phi{}^r$, respectively; and

the recovering step applies the Chinese remainder theorem to the residues $M_{p\,k}$, $M_{q\,\ell}$ and $M_{r\,m}$.

7. The method of claim 5, wherein the ciphertext C is obtained using the first secret key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by a product $p^k q$ where k = k1;

the obtaining step obtains a residue $K_{\emptyset}$ modulo p and a residue M_q modulo q of the plaintext M, by integer modular exponent calculations of:

$$K_{\emptyset} := C^{dp} \pmod{p}; \text{ and}$$

$$M_q := C^{dp} \pmod{q};$$

where:

$$dp := d \pmod{p-1}; \text{ and}$$

$$dq := d \pmod{q-1};$$

and obtains a residue M_{pk} modulo p^k of the plaintext M by applying the prescribed loop calculation to $K_{\emptyset}$; and the recovering steps applies the Chinese remainder theorem to the residues M_{pk} and M_q.

8. The method of claim 7, wherein the prescribed loop calculation is carried out by:

(a) setting $A_{\emptyset} := K_{\emptyset}$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$F_i := (A_{i-1}^e) \pmod{p^{i+1}};$$
$$E_i := (C - F_i) \pmod{p^{i+1}};$$
$$B_i := E_i / p^i \text{ in } Z;$$
$$K_i := ((eF_i)^{-1} A_{i-1} B_i) \pmod{p};$$
$$A_i := A_{i-1} + p^i K_i \text{ in } Z; \text{ and}$$

(c) setting $M_{pk} := A_{k-1}$.

9. The method of claim 7, wherein the recovering step recovers the plaintext M by calculating:

$$q_1 := q^{-1} \pmod{p^k};$$

$$v_1 := ((M_{pk} - M_q) q_1) \pmod{p^k}; \text{ and}$$

$$M := (M_q + q v_1).$$

10. The method of claim 7, wherein the recovering step recovers the plaintext M by calculating:

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$v_1 := ((M_q - M_{pk}) p_1) \pmod{q}; \text{ and}$$

$$M := (M_{pk} + p^k v_1).$$

11. The method of claim 7, wherein the recovering step recovers the plaintext M by calculating:

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$q_1 := q^{-1} \pmod{p^k}; \text{ and}$$

$$M := (q_1 q M_{pk} + p_1 p^k M_q) \pmod{p^k q}.$$

12. An authentication method for authenticating an authentication message sent from a sender to a receiver, compris-

ing the steps of:

(a) setting at the sender side a first secret key given by N (≧ 2) prime numbers p_1 , p_2, · · · · · · · · , p_N , a first public key n given by a product $p_1^{k1} p_2^{k2} \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot p_N^{kN}$ where k1, k2, · · · · · · · · , kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, · · · · · · · · , p_N-1;
(b) obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h;
(c) obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, · · · · · · · · , $h(C)_{pNkN}$ modulo p_1^{k1} , p_2^{k2} , · · · · · · · · , p_N^{kN} , respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first secret key p_1 , p_2 , · · · · · · · · , p_N , and applying Chinese remainder theorem to the residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, · · · · · · · · , $h(C)_{pNkN}$;
(d) sending the encrypted authenticator h(C) and the authentication message M from the sender to the receiver;
(e) obtaining at the receiver side a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from the encrypted authenticator h(C) received from the sender using the second public key e;
(f) obtaining at the receiver side a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h; and
(g) judging an authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

13. The method of claim 12, wherein the encrypted authenticator h(C) is obtained using the first secret key given by three prime numbers $p_1 = p$, $p_2 = q$ and $p_3 = r$ and the first public key n given by a product $p^k q^\ell r^m$ where k = k1, ℓ = k2 and m = k3 ;

the step (c) obtains $h(K)_\emptyset^{\ p}$, $h(K)_\emptyset^{\ q}$ and $h(K)_\emptyset^{\ r}$ modulo p, q and r, respectively, by integer modular exponent calculations of:

$$h(K)_\emptyset^{\ p} := h(M)^{dp} \pmod{p};$$

$$h(K)_\emptyset^{\ q} := h(M)^{dq} \pmod{q}; \text{ and}$$

$$h(K)_\emptyset^{\ r} := h(M)^{dr} \pmod{r};$$

where:

$$dp := d \pmod{p-1};$$

$$dq := d \pmod{q-1}; \text{ and}$$

$$dr := d \pmod{r-1};$$

and then obtaining the residues $h(C)_{pk}$, $h(C)_{q\ell}$ and $h(C)_{rm}$ modulo p^k , q^ℓ and r^m , respectively, by applying the prescribed loop calculation to $h(K)_\emptyset^{\ p}$, $h(K)_\emptyset^{\ q}$ and $h(K)_\emptyset^{\ r}$, respectively, and applies the Chinese remainder theorem to the residues $h(C)_{pk}$, $h(C)_{q\ell}$ and $h(C)_{rm}$.

14. The method of claim 12, wherein the encrypted authenticator h(C) is obtained using the first secret key given by two prime numbers $p_1 = p$ and $p_2 = q$ and the first public key n given by a product $p^k q$ where k = k1;

the step (c) obtains a residue $h(K)_\emptyset$ modulo p and a residue $h(C)_q$ modulo q of the encrypted authenticator h(C), by integer modular exponent calculations of:

$$h(K)_{\emptyset} := h(M)^{dp} \pmod{p}; \text{ and}$$

$$h(C)_q := h(M)^{dq} \pmod{q};$$

where:

$$dp := d \pmod{p-1}; \text{ and}$$

$$dq := d \pmod{q-1};$$

and obtains a residue $h(C)_{pk}$ modulo p^k of the encrypted authenticator h(C) by applying the prescribed loop calculation to $h(K)_{\emptyset}$, and applies the Chinese remainder theorem to the residues $h(C)_{pk}$ and $h(C)_q$.

15. The method of claim 14, wherein the prescribed loop calculation is carried out by:

(a) setting $h(A)_{\emptyset} := h(K)_{\emptyset}$;
(b) for i = 1 to (k-1), repeatedly calculating:

$$h(F)_i := (h(A)_{i-1}^e) \pmod{p^{i+1}};$$
$$h(E)_i := (h(M) - h(F)_i) \pmod{p^{i+1}};$$
$$h(B)_i := h(E)_i / p^i \text{ in } Z;$$
$$h(K)_i := ((eh(F)_i)^{-1} h(A)_{i-1} h(B)_i) \pmod{p};$$
$$h(A)_i := h(A)_{i-1} + p^i h(K)_i \text{ in } Z; \text{ and}$$

(c) setting $h(C)_{pk} := h(A)_{k-1}$.

16. The method of claim 14, wherein the step (c) applies the Chinese remainder theorem by calculating:

$$q_1 := q^{-1} \pmod{p^k};$$

$$v_1 := ((h(C)_{pk} - h(C)_q) q_1) \pmod{p^k}; \text{ and}$$

$$h(C) := (h(C)_q + q v_1).$$

17. The method of claim 14, wherein the step (c) applies the Chinese remainder theorem by calculating:

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$v_1 := ((h(C)_q - h(C)_{pk}) p_1) \pmod{q}; \text{ and}$$

$$h(C) := (h(C)_{pk} + p^k v_1).$$

18. The method of claim 14, wherein the step (c) applies the Chinese remainder theorem by calculating:

$$p_1 := (p^k)^{-1} \pmod{q};$$

$$q_1 := q^{-1} \pmod{p^k}; \text{ and}$$

$$h(C) := (q_1 q h(C)_{pk} + p_1 p^k h(C)_q) \pmod{p^k q}.$$

19. An encryption apparatus, comprising:

an encryption/decryption key generation processing unit for setting N (≧ 2) prime numbers p_1, p_2, ·····, p_N as a first secret key, and a product $p_1^{k1} p_2^{k2} \cdots\cdots p_N^{kN}$ as a first public key n,

where k1, k2, ・・・・・・・・・, kN are arbitrary positive integers, and determining a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・・, p_N-1, using the first secret key; and
an encryption processing unit for obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e.

20. A decryption apparatus for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using a first secret key given by N (≧ 2) prime numbers p_1, p_2, ・・・・・・・・・, p_N, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, ・・・・・・・・・, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・・, p_N-1, the apparatus comprising:

a calculation processing unit for obtaining residues M_{p1k1}, M_{p2k2}, ・・・・・・・・・, M_{pNkN} modulo p_1^{k1}, $p_2^{k2} \cdots\cdots\cdots p_N^{kN}$, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key p_1, p_2, ・・・・・・・・・, p_N; and
a decryption processing unit for recovering the plaintext M by applying Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ・・・・・・・・・, M_{pNkN}.

21. A cipher communication system, comprising:

a sender apparatus having:

an encryption/decryption key generation processing unit for setting N (≧ 2) prime numbers p_1, p_2, ・・・・・・・・・, p_N as a first secret key, and a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ as a first public key n, where k1, k2, ・・・・・・・・・, kN are arbitrary positive integers, and determining a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・・, p_N-1, using the first secret key; and
an encryption processing unit for obtaining a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e; and

a receiver apparatus having:

a calculation processing unit for obtaining residues M_{p1k1}, M_{p2k2}, ・・・・・・・・・, M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ・・・・・・・・・, p_N^{kN}, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key p_1, p_2, ・・・・・・・・・, p_N; and
a decryption processing unit for recovering the plaintext M by applying Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ・・・・・・・・・, M_{pNkN}.

22. An authentication message sender apparatus for use in authenticating an authentication message sent from a sender to a receiver, the apparatus comprising:

an encryption/decryption key generation processing unit for setting at the sender side a first secret key given by N (≧ 2) prime numbers p_1 , p_2 , ・・・・・・・・ , p_N , a first public key n given by a product p_1^{k1} p_2^{k2} ・・・・・・・・ p_N^{kN} where k1, k2, ・・・・・・・・ , kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・ , p_N-1;
an authentication message hashing processing unit for obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and
an authenticator encryption processing unit for obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ・・・・・・・・ , $h(C)_{pNkN}$ modulo p_1^{k1} , p_2^{k2} , ・・・・・・・・ , p_N^{kN} , respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first secret key p_1 , p_2 , ・・・・・・・・ , p_N, and applying Chinese remainder theorem to the residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ・・・・・・・・ , $h(C)_{pNkN}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver.

23. An authentication message receiver apparatus for use in authenticating an authentication message sent from a sender to a receiver, using a first secret key given by N (≧ 2) prime numbers p_1 , p_2, ・・・・・・・・ , p_N , a first public key n given by a product p_1^{k1} p_2^{k2} ・・・・・・・・ p_N^{kN} where k1, k2, ・・・・・・・・ , kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・ , p_N-1, the apparatus comprising:

an authenticator decryption processing unit for obtaining a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from an encrypted authenticator h(C) received from the sender using the second public key e;
an authentication message hashing processing unit for obtaining a second authenticator $h(M)_2$ by hashing an authentication message M received from the sender using a hash function h; and
an authenticity verification processing unit for judging an authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

24. An authentication system for authenticating an authentication message sent from a sender to a receiver, the system comprising:

a sender apparatus having:

an encryption/decryption key generation processing unit for setting at the sender side a first secret key given by N (≧ 2) prime numbers p_1 , p_2 , ・・・・・・・・ , p_N , a first public key n given by a product p_1^{k1} p_2^{k2} ・・・・・・・・ p_N^{kN} where k1, k2, ・・・・・・・・ , kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・ , p_N-1;
an authentication message hashing processing unit for obtaining at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and
an authenticator encryption processing unit for obtaining at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ·····, $h(C)_{pNkN}$ modulo p_1^{k1}, p_2^{k2}, ····· , p_N^{kN}, respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first secret key p_1, p_2, ····· ,p_N, and applying Chinese remainder theorem to the residues $h(C)_{p1k1}$, $h(C)_{p2k2}$, ····· , $h(C)_{pNkN}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver; and

a receiver apparatus having:

an authenticator decryption processing unit for obtaining a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from the encrypted authenticator h(C) received from the sender using the second public key e;
an authentication message hashing processing unit for obtaining a second authenticator $h(M)_2$ by hashing the authentication message M received from the sender using the hash function h; and
an authenticity verification processing unit for judging an authenticity of the authentication message M by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

25. A computer usable medium having computer readable program code means embodied therein for causing a computer to function as an encryption apparatus, the computer readable program code means includes:

first computer readable program code means for causing said computer to set N (≧ 2) prime numbers p_1, p_2, ····· , p_N as a first secret key, and a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ as a first public key n, where k1, k2, ····· , kN are arbitrary positive integers, and determining a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ····· , p_N-1, using the first secret key; and
second computer readable program code means for causing said computer to obtain a ciphertext C from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using the first public key n and the second public key e.

26. A computer usable medium having computer readable program code means embodied therein for causing a computer to function as a decryption apparatus for decrypting a ciphertext C obtained from a plaintext M according to:

$$C \equiv M^e \pmod{n}$$

using a first secret key given by N (≧ 2) prime numbers p_1, p_2, ····· , p_N, first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots\cdots p_N^{kN}$ where k1, k2, ····· , kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ····· , p_N-1, the computer readable program code means includes:

first computer readable program code means for causing said computer to obtain residues M_{p1k1}, M_{p2k2}, ····· , M_{pNkN} modulo p_1^{k1}, p_2^{k2}, ····· , p_N^{kN}, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key p_1, p_2, ····· , p_N; and
second computer readable program code means for causing said computer to recover the plaintext M by applying Chinese remainder theorem to the residues M_{p1k1}, M_{p2k2}, ····· , M_{pNkN}.

27. A computer usable medium having computer readable program code means embodied therein for causing a computer to function as an authentication message sender apparatus for use in authenticating an authentication message sent from a sender to a receiver, the computer readable program code means includes:

first computer readable program code means for causing said computer to set at the sender side a first secret

key given by N (≧ 2) prime numbers p_1 , p_2 , ・・・・・・・・ , p_N , a first public key n given by a product p_1^{k1} p_2^{k2} ・・・・・・・・ p_N^{kN} where k1, k2, ・・・・・・・・ , kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・ , p_N-1;
second computer readable program code means for causing said computer to obtain at the sender side an authenticator h(M) by hashing the authentication message M using a hash function h; and
third computer readable program code means for causing said computer to obtain at the sender side an encrypted authenticator h(C) of the authenticator h(M) according to:

$$h(M) \equiv h(C)^e \pmod{n}$$

by obtaining residues $h(C)_{p\,1\,k\,1}$, $h(C)_{p\,2\,k\,2}$, ・・・・・・・・ , $h(C)_{p\,N\,k\,N}$ modulo p_1^{k1} , p_2^{k2} , ・・・・・・・・ , p_N^{kN} , respectively, of the encrypted authenticator h(C) using a prescribed loop calculation with respect to the first secret key p_1 , p_2 , ・・・・・・・・ , p_N , and applying Chinese remainder theorem to the residues $h(C)_{p\,1\,k\,1}$, $h(C)_{p\,2\,k\,2}$, ・・・・・・・・ , $h(C)_{p\,N\,k\,N}$, and then sending the encrypted authenticator h(C) and the authentication message M to the receiver.

28. A computer usable medium having computer readable program code means embodied therein for causing a computer to function as an authentication message receiver apparatus for use in authenticating an authentication message sent from a sender to a receiver, using a first secret key given by N (≧ 2) prime numbers p_1 , p_2 , ・・・・・・・・ , p_N , a first public key n given by a product p_1^{k1} p_2^{k2} ・・・・・・・・ p_N^{kN} where k1, k2, ・・・・・・・・ , kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy:

$$ed \equiv 1 \pmod{L}$$

where L is a least common multiple of p_1-1, p_2-1, ・・・・・・・・ , p_N-1, the computer readable program code means includes:

first computer readable program code means for causing said computer to obtain a first authenticator $h(M)_1$ by calculating $h(C)^e$ (mod n) from an encrypted authenticator h(C) received from the sender using the second public key e;
second computer readable program code means for causing said computer to obtain a second authenticator $h(M)_2$ by hashing an authentication message M received from the sender using a hash function h; and
third computer readable program code means for causing said computer to judge an authenticity of the authentication message M at the receiver side by checking whether the first authenticator $h(M)_1$ and the second authenticator $h(M)_2$ coincide or not.

FIG. 1

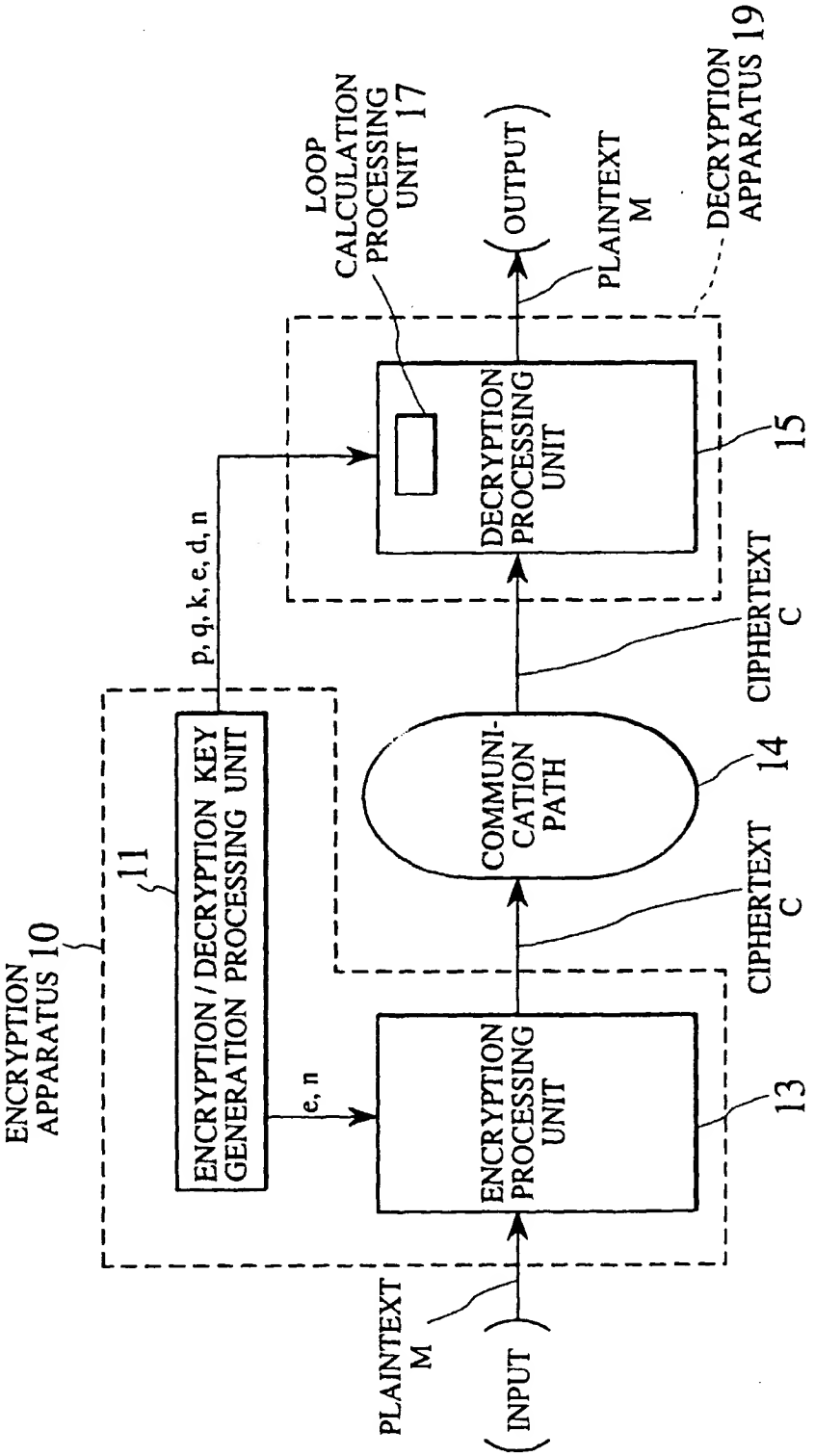

ENCRYPTION APPARATUS 10
11
ENCRYPTION / DECRYPTION KEY GENERATION PROCESSING UNIT
p, q, k, e, d, n
e, n
ENCRYPTION PROCESSING UNIT
13
CIPHERTEXT C
COMMUNI-CATION PATH
14
CIPHERTEXT C
DECRYPTION PROCESSING UNIT
15
LOOP CALCULATION PROCESSING UNIT 17
DECRYPTION APPARATUS 19
PLAINTEXT M
(OUTPUT)
PLAINTEXT M
(INPUT)

FIG. 2

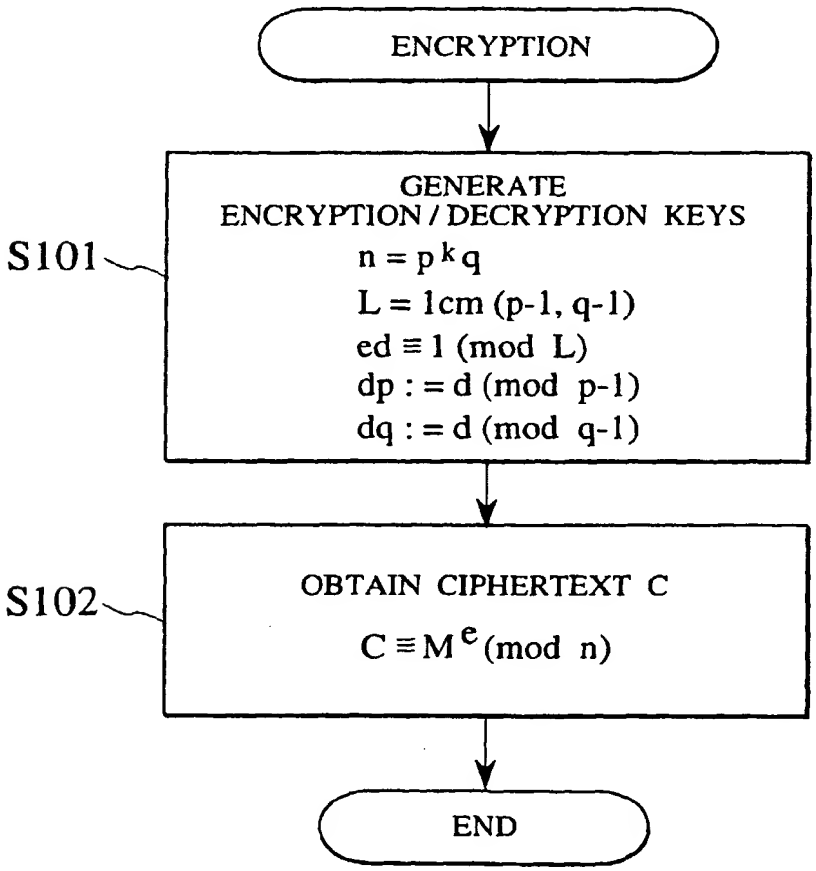


FIG. 3

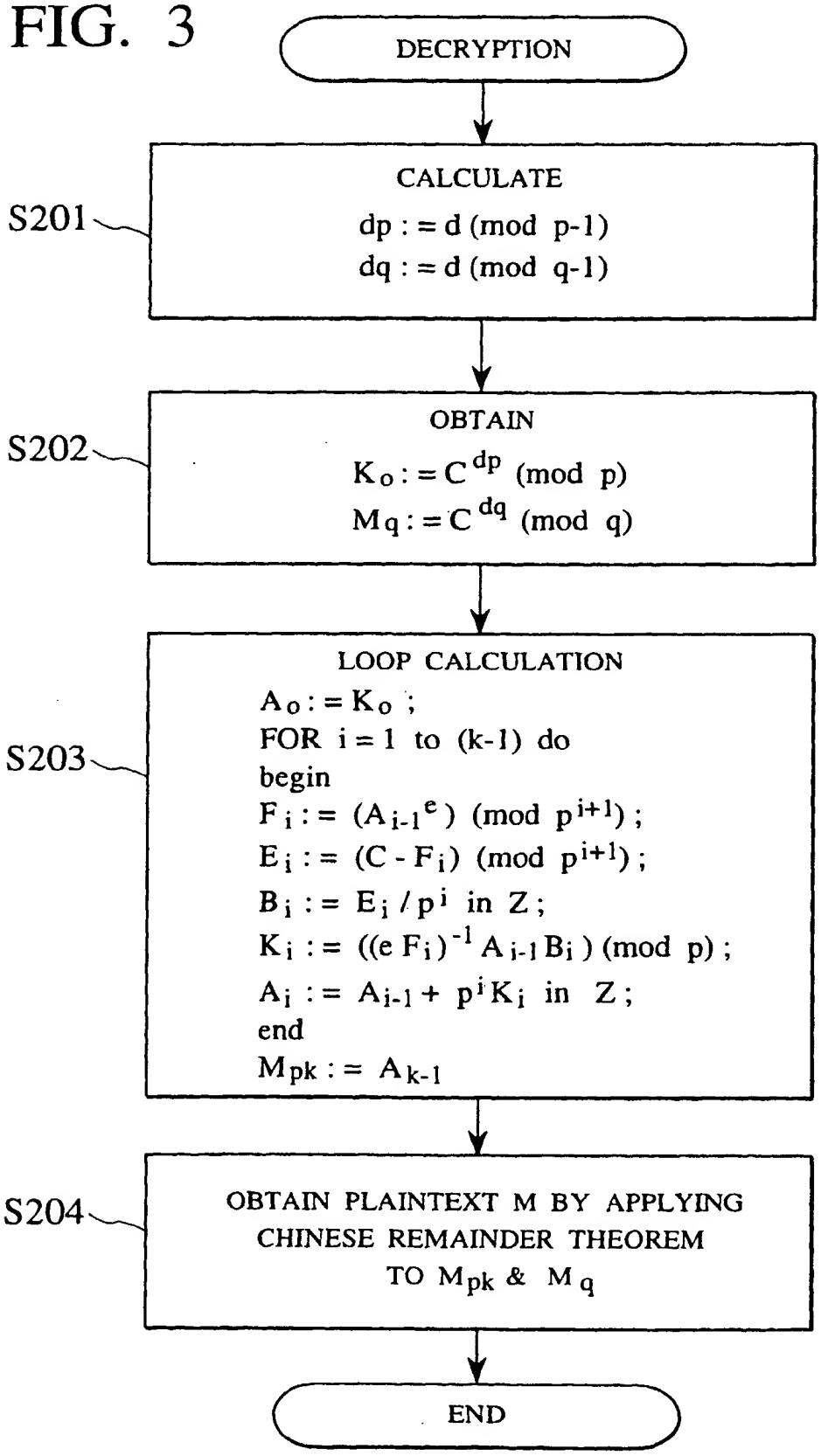


FIG. 4

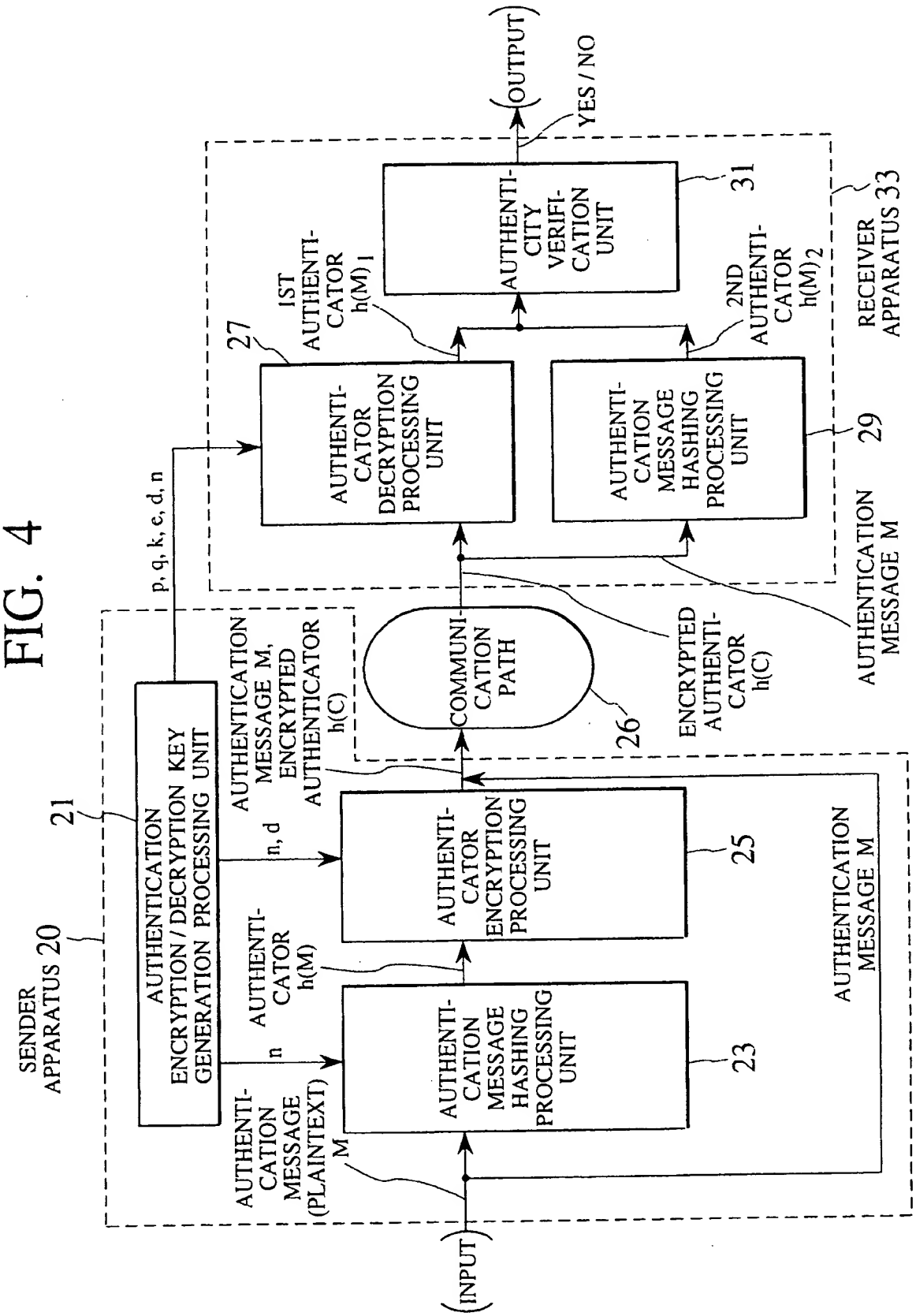
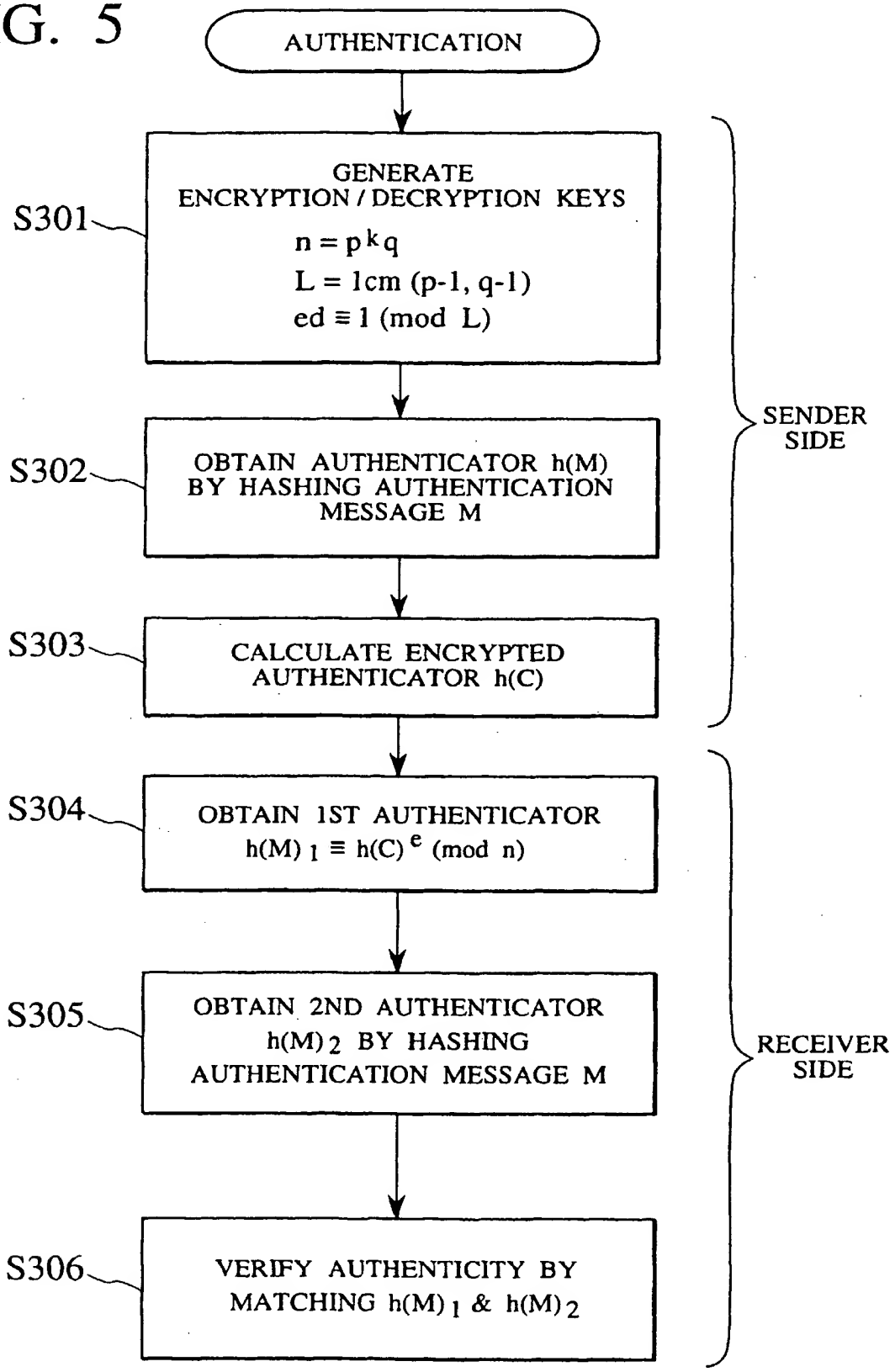


FIG. 5



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 946 018 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
14.08.2002 Bulletin 2002/33

(43) Date of publication A2:
29.09.1999 Bulletin 1999/39

(21) Application number: **99105099.8**

(22) Date of filing: **25.03.1999**

(51) Int Cl.[7]: **H04L 9/30**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **26.03.1998 JP 7983698**
21.08.1998 JP 23608498

(71) Applicant: **Nippon Telegraph and Telephone Corporation**
Tokyo (JP)

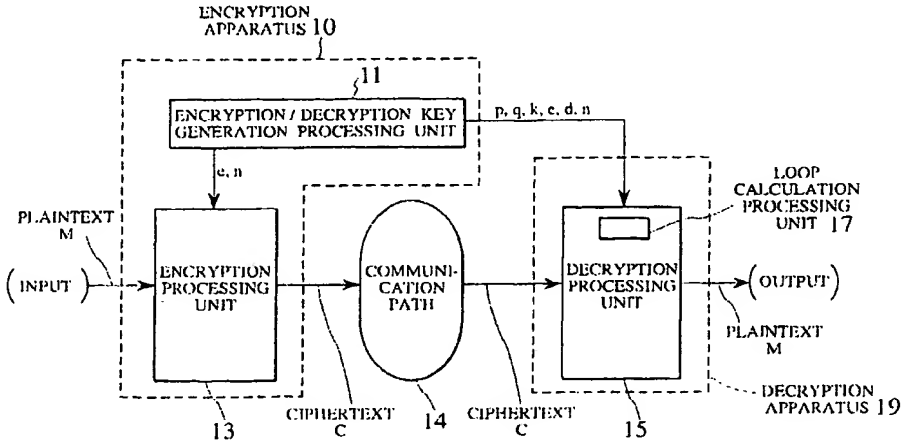
(72) Inventors:
- **Takagi, Tsuyoshi, c/o Nippon T.& T. Corporation**
Shinjuku-ku, Tokyo 163-14 (JP)
- **Naito, Shozo, c/o Nippon T. & T. Corporation**
Shinjuku-ku, Tokyo 163-14 (JP)

(74) Representative: **HOFFMANN - EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) Scheme for fast realization of encryption, decryption and authentication

(57) A new scheme for fast realization of encryption, decryption and authentication which can overcome the problems of the RSA cryptosystem is disclosed. The encryption obtains a ciphertext C from a plaintext M according to $C \equiv M^e \pmod n$ using a first secret key given by N ($\geqq 2$) prime numbers $p_1, p_2, \cdots\cdots, p_N$, a first public key n given by a product $p_1^{k1} p_2^{k2} \cdots\cdots p_N^{kN}$ where k1, k2, ·····, kN are arbitrary positive integers, a second public key e and a second secret key d which satisfy $ed \equiv 1 \pmod L$ where L is a least common multiple of $p_1-1, p_2-1, \cdots\cdots, p_N-1$. The decryption recovers the plaintext M by obtaining residues $M_{p1k1}, M_{p2k2}, \cdots\cdots, M_{pNkN}$ modulo $p_1^{k1}, p_2^{k2}, \cdots\cdots, p_N^{kN}$, respectively, of the plaintext M using a prescribed loop calculation with respect to the first secret key $p_1, p_2, \cdots\cdots, p_N$, and by applying the Chinese remainder theorem to the residues $M_{p1k1}, M_{p2k2}, \cdots\cdots, M_{pNkN}$. This encryption/decryption scheme can be utilized for realizing the authentication.

FIG. 1



EP 0 946 018 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 10 5099

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	WO 90 02456 A (NCR CO) 8 March 1990 (1990-03-08) * page 1, line 1 - line 20 * * page 5, line 14 - page 6, line 4 *	1-4,19, 25	H04L9/30
A	FRANKEL Y ET AL: "PROACTIVE RSA" , ADVANCES IN CRYPTOLOGY - CRYPTO '97. SANTA BARBARA, AUG. 17 - 21, 1997, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, VOL. CONF. 17, PAGE(S) 440-454 XP000767549 ISBN: 3-540-63384-7 * page 443, line 37 - line 40 *	1-28	
A	EP 0 381 523 A (TOKYO SHIBAURA ELECTRIC CO) 8 August 1990 (1990-08-08) * page 2, line 25 - page 3, line 7 *	4-18, 20-24, 26,27	
A	BRUCE SCHNEIER: "Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition" 1996 , JOHN WILEY & SONS, INC. , NEW YORK XP002201616 * page 249 - page 250 *	4-18, 20-24, 26,27	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L
A	EP 0 823 802 A (NIPPON TELEGRAPH & TELEPHONE) 11 February 1998 (1998-02-11) * page 2, line 1 - page 3, line 38 * * page 30, line 39 - page 31, line 35 *	7,8	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	11 June 2002	Liebhardt, I

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 10 5099

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X,P	TAKAGI T: "FAST RSA-TYPE CRYPTOSYSTEM MODULO PKQ" , ADVANCES IN CRYPTOLOGY. CRYPTO '98. 18TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 23 - 27, 1998. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1462, BERLIN: SPRINGER, DE, PAGE(S) 318-326 XP000792177 ISBN: 3-540-64892-5 * the whole document * ---	1,3-5, 7-28	
X,P	WO 98 26536 A (TANDEM COMPUTERS INC) 18 June 1998 (1998-06-18) * page 5, line 8 - page 6, line 9 * * page 8, line 8 - page 9, line 32 * * claims 1,2,4,5 * -----	1-8, 19-21, 25,26	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	11 June 2002	Liebhardt, I

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 10 5099

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

11-06-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9002456 A	08-03-1990	AU 607351 B2	28-02-1991
		AU 4052489 A	23-03-1990
		CA 1321835 A1	31-08-1993
		DE 68907717 D1	26-08-1993
		DE 68907717 T2	17-02-1994
		DE 400103 T1	28-02-1991
		EP 0400103 A1	05-12-1990
		JP 3505033 T	31-10-1991
		WO 9002456 A1	08-03-1990
		US 4944007 A	24-07-1990
EP 0381523 A	08-08-1990	JP 2204768 A	14-08-1990
		JP 3137190 B2	19-02-2001
		JP 3053367 A	07-03-1991
		EP 0381523 A2	08-08-1990
		US 5046094 A	03-09-1991
		JP 3073990 A	28-03-1991
		JP 3072737 A	27-03-1991
EP 0823802 A	11-02-1998	JP 11065439 A	05-03-1999
		CA 2212664 A1	09-02-1998
		EP 0823802 A2	11-02-1998
		US 6259790 B1	10-07-2001
WO 9826536 A	18-06-1998	US 5848159 A	08-12-1998
		AU 5689398 A	03-07-1998
		EP 0950302 A1	20-10-1999
		JP 2001510583 T	31-07-2001
		WO 9826536 A1	18-06-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82